



(12) BẢN MÔ TẢ SÁNG CHẾ THUỘC BẢNG ĐỘC QUYỀN SÁNG CHẾ

(19) Cộng hòa xã hội chủ nghĩa Việt Nam (VN)
CỤC SỞ HỮU TRÍ TUỆ

(11) 
1-0021109

(51)⁷ G06F 29, G06K 9

(13) B

(21) 1-2016-04284

(22) 08.11.2016

(45) 25.06.2019 375

(43) 25.04.2017 349

(73) CÔNG TY CỔ PHẦN CÔNG NGHỆ HỘI TỤ UCONSYS (VN)

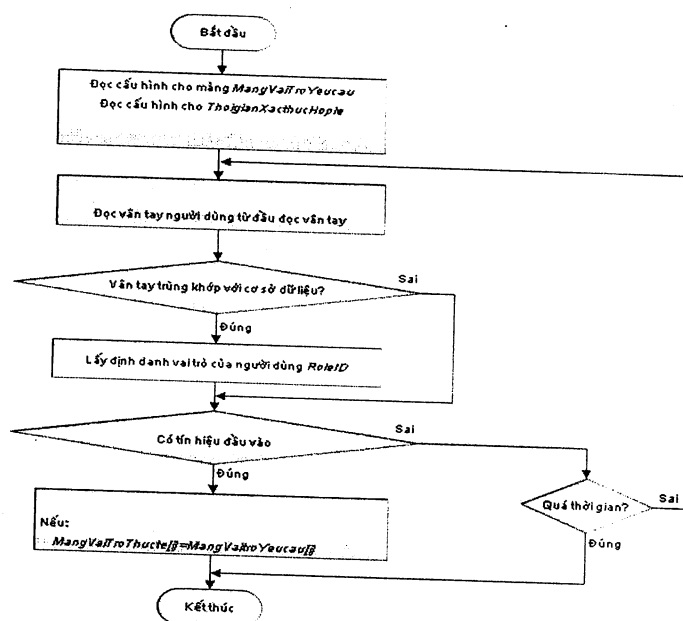
Nhà số 3, tổ 6, cụm 1, phường Khương Đình, quận Thanh Xuân, thành phố Hà Nội

(72) Hà Hải Nam (VN)

(74) Công ty TNHH SHARETOLINK Việt Nam (VN SHARETOLINK COMPANY LIMITED)

(54) HỆ THỐNG ĐIỀU KHIỂN TRUY CẬP THÔNG QUA QUY TRÌNH XÁC THỰC VÂN TAY ĐỒNG THỜI NHIỀU NGƯỜI DÙNG VỚI NHIỀU VAI TRÒ KHÁC NHAU

(57) Sáng chế đề xuất hệ thống điều khiển truy cập thông qua quy trình xác thực vân tay có thể thiết lập điều kiện xác thực nhiều người dùng với nhiều vai trò khác nhau đồng thời trong một phiên xác thực. Hệ thống theo sáng chế khác biệt với các hệ thống tương ứng đã biết ở chỗ, hệ thống cho phép thiết lập điều kiện xác thực hợp lệ khi đồng thời nhiều người dùng với nhiều vai trò đồng thời được xác thực bằng vân tay. Ngoài ra, hệ thống theo sáng chế còn thực hiện việc làm bất hợp lệ phiên xác thực nếu thời gian thực hiện xác thực lâu hơn một khoảng thời gian định trước. Hệ thống này còn có khả năng kích hoạt việc cảnh báo cục bộ và cảnh báo trung tâm. Hệ thống này đảm bảo mức độ an toàn xác thực cao, đồng thời cũng cho phép mức độ tùy chỉnh cao và đảm bảo an toàn dữ liệu khi mất nguồn điện hệ thống.



Lĩnh vực kỹ thuật được đề cập

Sáng chế liên quan đến lĩnh vực xác thực sử dụng công nghệ sinh trắc học vân tay đồng thời nhiều người dùng với nhiều vai trò khác nhau.

Tình trạng kỹ thuật của sáng chế

Hiện nay trong các hệ thống truy cập yêu cầu xác thực sử dụng vân tay, người sử dụng hệ thống có đăng ký vân tay trong cơ sở dữ liệu của hệ thống và sử dụng vân tay làm công cụ xác thực nhận diện cá nhân của người dùng.

Các hệ thống hiện có trên thị trường về cấu tạo cơ bản gồm hai thành phần: phần mềm quản lý vân tay và thiết bị phần cứng thu nhận vân tay và xác thực vân tay. Các hệ thống hiện có trên thị trường chỉ có khả năng xác thực theo điều kiện đơn giản bằng cách so sánh một vân tay của một người dùng với cơ sở dữ liệu vân tay trên thiết bị và nếu vân tay của người dùng trùng khớp với vân tay có trong cơ sở dữ liệu vân tay trên thiết bị thì điều kiện xác thực được cho là hợp lệ. Hệ thống hiện có không cho phép thiết lập điều kiện xác thực kết hợp như kết hợp nhiều người dùng với nhiều vai trò đồng thời trong một phiên xác thực.

Bản chất kỹ thuật của sáng chế

Mục đích của sáng chế là đề xuất hệ thống điều khiển truy cập thông qua quy trình xác thực vân tay có thể thiết lập điều kiện xác thực nhiều người dùng với nhiều vai trò khác nhau đồng thời trong một phiên xác thực. Hệ thống này đảm bảo mức độ an toàn xác thực cao hơn, đồng thời hệ thống cũng cho phép mức độ tùy chỉnh cao và đảm bảo an toàn dữ liệu khi mất nguồn điện hệ thống.

Theo một phương án sáng chế đề xuất hệ thống điều khiển truy cập thông qua quy trình xác thực vân tay có thể thiết lập điều kiện xác thực nhiều người dùng với nhiều vai trò khác nhau, hệ thống này bao gồm:

các thành phần phần cứng bao gồm:

bo mạch chủ xử lý bao gồm bộ chip vi điều khiển và các vi mạch IC phụ trợ thực hiện các chức năng giao tiếp mạng, điều khiển vào ra và giao tiếp với các đầu đọc vân tay, các thuật toán xử lý được lập trình và nạp vào trong bộ nhớ ở bên trong chip vi điều khiển;

mô đun đầu đọc vân tay được sử dụng để đọc vân tay và lưu giữ các vân tay của người sử dụng, các thuật toán so sánh các đặc trưng vân tay được cài đặt trong mô đun này;

màn hình hiển thị để hiển thị thông tin tương tác với người dùng;

loa của thiết bị để phát các âm thanh cảnh báo, âm bàn phím âm chỉ thị;

bàn phím dùng để nhập các thông tin và giúp người dùng tương tác với thiết bị phần cứng;

các cổng điều khiển vào ra dùng để điều khiển các thiết bị cảnh báo bên ngoài và nhận tín hiệu điều khiển đầu vào;

cổng giao tiếp mạng dùng để cắm dây mạng để kết nối thiết bị vào mạng truyền thông;

máy chủ trung tâm được cài đặt ứng dụng giao diện web, truyền thông qua mạng với bo mạch chủ xử lý để có thể giám sát và cấu hình từ xa bo mạch chủ và các thiết bị phần cứng khác;

thành phần phần mềm được cài đặt trong các thành phần phần cứng tương ứng để thực hiện các bước sau đây:

xác thực hợp lệ khi đồng thời nhiều người dùng với nhiều vai trò đồng thời được xác thực bằng vân tay thực hiện thông qua thuật toán được cài đặt trong phần sụn (firmware) của thiết bị phần cứng xác thực vân tay, trong đó:

mỗi người dùng được gán một vai trò xác định đại diện bởi định danh của vai trò, định danh của vai trò là một số nguyên dương nhận giá trị trong khoảng từ 0 đến $N-1$, trong đó N là một số nguyên dương được cấu hình trước,

danh sách vai trò yêu cầu cho việc xác thực hợp lệ là một mảng N phần tử gọi là `MangVaitroYeucan`, trong đó mỗi phần tử nhận một trong hai giá trị đúng (True) hoặc sai (False), giá trị True của một phần tử có nghĩa là vai trò có định danh tương ứng là chỉ số mảng của phần tử đó cần trong xác thực hợp lệ, giá trị False của một phần tử có nghĩa là vai trò có định danh tương ứng là chỉ số mảng của phần tử đó không cần trong xác thực hợp lệ, giá trị của các phần tử trong `MangVaitroYeucan` được định nghĩa trước tùy thuộc vào yêu cầu của từng hệ thống,

danh sách vai trò thực tế có được trong một phiên xác thực là một mảng N phần tử gọi là `MangVaitroThucte`, trong đó mỗi phần tử nhận một trong hai giá trị True hoặc False, khi bắt đầu một phiên xác thực, các phần tử của mảng `MangVaitroThucte` được thiết lập về giá trị False, trong một phiên xác thực, nếu một người dùng xác thực có vân tay trùng khớp trong cơ sở dữ liệu, thì định danh tương ứng của vai trò của người dùng (RoleID) được dùng làm chỉ số mảng để cập nhật

phần tử tương ứng của mảng MangVaitroThucte thành giá trị True (MangVaitroThucte[RoleID] = True), khi nhận được tín hiệu điều khiển đầu vào kết thúc phiên xác thực, hai mảng MangVaitroYeucan và mảng MangVaitroThucte được so sánh với nhau, nếu 2 mảng có tất cả các phần tử giống nhau thì phiên xác thực là hợp lệ; và

làm bất hợp lệ phiên xác thực sau một khoảng thời gian cho trước, trong đó thời gian xác thực hợp lệ cho một phiên xác thực được cấu hình trước và lưu trong bộ nhớ của thiết bị.

Theo một khía cạnh của phương án này, khi điều kiện xác thực không hợp lệ, hệ thống điều khiển truy cập theo sáng chế còn kích hoạt tín hiệu đầu ra điều khiển thiết bị cảnh báo cục bộ và gửi bản tin cảnh báo đến ứng dụng được cài đặt ở máy chủ trung tâm, bản tin cảnh báo này chứa thông tin về vị trí cảnh báo, người dùng truy cập, thời gian xảy cảnh báo, trạng thái đầu vào khác, việc gửi bản tin được thực hiện bằng cách truyền thông sử dụng một hoặc một số giao thức truyền thông chuẩn phổ biến bao gồm TCP, UDP, HTTP, dịch vụ web RESTful (RESTful Web Services).

Theo một khía cạnh khác của phương án này, hệ thống điều khiển truy cập theo sáng chế có chức năng ghi thông tin theo dõi cục bộ trong bộ nhớ của bo mạch chủ xử lý, thông tin này là thông tin về các lần truy cập thiết bị trong trường hợp mất kết nối truyền thông, khi có kết nối truyền thông, thiết bị tự động gửi các thông tin đã lưu lên ứng dụng được cài đặt trên máy chủ trung tâm.

Theo một khía cạnh khác của phương án này, hệ thống điều khiển truy cập theo sáng chế có chức năng hỗ trợ tối đa 8 vân tay cho mỗi người dùng.

Theo một khía cạnh khác của phương án này, hệ thống điều khiển truy cập theo sáng chế có thể hỗ trợ tối đa 100 người dùng.

Theo một khía cạnh khác của phương án này, hệ thống điều khiển truy cập theo sáng chế có chức năng thêm, sửa, xóa, gán vai trò người dùng.

Theo một khía cạnh khác của phương án này, hệ thống điều khiển truy cập theo sáng chế có chức năng đăng ký liên tục nhiều vân tay cho một người dùng và nhiều người dùng trong một phiên đăng ký.

Theo một khía cạnh khác của phương án này, hệ thống điều khiển truy cập theo sáng chế còn có chức năng bảo mật bằng mật khẩu, hệ thống này yêu cầu mật khẩu khi người dùng truy cập các chức năng cấu hình và mật khẩu có thể thay đổi được bởi người dùng quản trị thông qua bàn phím trên thiết bị hoặc thông qua giao diện quản trị web.

Theo một khía cạnh khác của phương án này, hệ thống điều khiển truy cập theo sáng chế còn cung cấp chức năng cấu hình thông qua giao diện web cho phép cấu hình từ xa thiết bị, các tham số cấu hình bao gồm: địa chỉ MAC, địa chỉ IP, mức bảo mật, mở/ khóa bàn phím thiết bị, cho phép/không cho phép tắt tín hiệu đầu ra điều khiển cảnh báo trên bàn phím thiết bị, thiết lập thời gian hệ thống, thiết lập khoảng thời gian tối đa cho phiên xác thực.

Theo một khía cạnh khác của phương án này, hệ thống điều khiển truy cập theo sáng chế còn có chức năng bảo toàn dữ liệu khi mất điện, các dữ liệu cấu hình, người dùng, thông tin theo dõi cảnh báo vẫn tồn tại khi mất nguồn điện cấp cho thiết bị.

Theo một khía cạnh khác của phương án này, hệ thống điều khiển truy cập theo sáng chế có chức năng kiểm tra tình trạng kết nối mạng của các thiết bị phần cứng khác khác như bo mạch chủ xử lý, camera, máy tính, v.v..

Mô tả vắn tắt các hình vẽ

Sáng chế sẽ được mô tả chi tiết có dựa vào các hình vẽ kèm theo, trong đó:

Hình 1 là hình vẽ thể hiện sơ đồ kiến trúc tổng quan của hệ thống điều khiển truy cập thông qua quy trình xác thực vân tay nhiều người dùng với nhiều vai trò khác nhau theo sáng chế;

Hình 2 là hình vẽ thể hiện mối quan hệ tương tác giữa các thành phần của thiết bị phần cứng của hệ thống theo sáng chế;

Hình 3 là hình vẽ lưu đồ thuật toán đảm bảo xác thực đa vai trò và bất hợp lệ phiên xác thực.

Mô tả chi tiết sáng chế

Trong hệ thống truy cập yêu cầu xác thực sử dụng vân tay theo sáng chế, người sử dụng hệ thống có đăng ký vân tay trong cơ sở dữ liệu của hệ thống và sử dụng vân tay làm công cụ xác thực nhận diện cá nhân của người dùng.

Liên quan đến vai trò của người dùng, mỗi người dùng sẽ có một vai trò xác định tùy thuộc vào tổ chức. Ví dụ: vai trò giám đốc, vai trò trưởng phòng, v.v..

Tiếp theo, các yếu tố xác thực là tập hợp các điều kiện mà hệ thống sẽ kiểm tra và kết quả của kiểm tra là thỏa mãn hoặc không thỏa mãn. Việc xác thực sẽ là hợp lệ khi tất cả các điều kiện của yếu tố xác thực được đồng thời thỏa mãn.

Trong hệ thống được sáng chế đề xuất, các điều kiện kiểm tra là:

- 1) Tất cả các vân tay của các người dùng trong phiên xác thực trùng khớp với vân tay trong cơ sở dữ liệu của thiết bị hay không?
- 2) Các người dùng trong phiên xác thực phải có đủ các vai trò đã được cấu hình hay không?

Một yếu tố khác của việc xác thực là phiên xác thực, đây là một quá trình trong đó các người dùng thực hiện kiểm tra xác thực hợp lệ với hệ thống. Quá trình xác thực được bắt đầu khi và kết thúc bởi các tín hiệu điều khiển kích hoạt đầu vào thiết bị như bàn phím, các cổng vào ra của thiết bị.

Ngoài ra, liên quan đến phiên xác thực, thời gian hợp lệ cho phiên xác thực là khoảng thời gian tối đa của phiên xác thực. Trong khoảng thời gian này các người dùng phải hoàn thành xác thực hợp lệ. Khoảng thời gian này có thể cấu hình được.

Như được thể hiện trên hình 1, hệ thống điều khiển truy cập thông qua quy trình xác thực vân tay đồng thời nhiều người dùng với nhiều vai trò khác nhau gồm hai thành phần: phần cứng thiết bị nhận dạng vân tay với phần sụn (firm ware) nạp trong chip vi điều khiển; và phần mềm quản lý hệ thống điều khiển truy cập đa vai trò bằng vân tay.

Phần cứng cho phép cấu hình nhiều người dùng với nhiều vai trò khác nhau. Truy cập hệ thống là hợp lệ khi đồng thời nhiều người dùng với đầy đủ các vai trò cùng truy cập xác thực bằng vân tay trong một khoảng thời gian cho trước cấu hình được. Các truy cập hệ thống không hợp lệ khi các người dùng xác thực không đủ các vai trò. Khi truy cập hệ thống không hợp lệ, phần cứng sẽ gửi cảnh báo thông qua kết nối mạng đến phần mềm trung tâm sử dụng giao thức truyền thông mạng chuẩn. Phần mềm trung tâm cho phép hiển thị cảnh báo, cấu hình người dùng, kết xuất báo cáo thống kê.

Theo một phương án làm ví dụ của sáng chế, phần cứng của hệ thống điều khiển truy cập theo sáng chế bao gồm các thành phần cơ bản như dưới đây.

Bộ mạch xử lý của hệ thống bao gồm bộ chip vi điều khiển và các vi mạch IC phụ trợ thực hiện các chức năng giao tiếp mạng IP (ví dụ, mạng Ethernet, LAN, WLAN, ...) điều khiển vào ra và giao tiếp với các đầu đọc vân tay. Các thuật toán xử lý được lập trình và nạp vào trong bộ nhớ ở bên trong chip vi điều khiển.

Đầu đọc vân tay được sử dụng để đọc vân tay và lưu giữ các vân tay của người sử dụng. Các thuật toán so sánh các đặc trưng vân tay được cài đặt trong mô đun này.

Màn hình hiển thị để hiển thị thông tin tương tác với người dùng. Màn hình này, ví dụ, có thể là một màn hình LCD hiển thị 4 hàng mỗi hàng 16 ký tự.

Loa của thiết bị để phát các âm thanh cảnh báo, âm bàn phím âm chỉ thị.

Bàn phím dùng để nhập các thông tin và giúp người dùng tương tác với thiết bị phần cứng. Bàn phím, ví dụ, có thể bao gồm 16 phím bao gồm các số từ 0 đến 9, OK, ESC, phím di chuyển con trỏ lên, phím di chuyển con trỏ xuống và phím tắt cảnh báo.

Các cổng điều khiển vào ra với mức điện áp logic mức TTL 0 hoặc 5 V dùng để điều khiển các thiết bị cảnh báo bên ngoài và nhận tín hiệu điều khiển đầu vào.

Cổng giao tiếp mạng dùng để cắm dây mạng để kết nối thiết bị vào mạng truyền thông.

Ngoài ra, mặc dù không thể hiện trên hình vẽ, nhưng phần cứng hệ thống theo sáng chế có thể còn bao gồm một máy chủ trung tâm được cài đặt ứng dụng giao diện web, truyền thông qua mạng với bo mạch chủ xử lý để có thể giám sát và cấu hình từ xa bo mạch chủ và các thiết bị phần cứng khác. Việc truyền thông giữa máy chủ trung tâm và bo mạch chủ xử lý có thể thông qua các phương tiện truyền có dây hoặc không dây, qua mạng IP (ví dụ, mạng Ethernet, LAN, WLAN, ...) hoặc không qua mạng.

Tiếp theo, hình 2 minh họa mối quan hệ giữa các thành phần của hệ thống điều khiển truy cập theo sáng chế. Trong đó, chiều của các mũi tên chỉ thị chiều điều khiển, truyền thông tín hiệu.

Các dấu hiệu của hệ thống điều khiển truy cập thông qua quy trình xác thực vân tay đồng thời nhiều người dùng với nhiều vai trò khác nhau theo sáng chế, có thể được hiểu rõ hơn thông qua phần phân tích các đặc điểm chức năng chính của hệ thống dưới đây.

1) Xác thực đa vai trò

Hệ thống theo sáng chế cho phép thiết lập điều kiện xác thực kết hợp nhiều vai trò của nhiều người dùng. Điều kiện xác thực là hợp lệ nếu trong cùng một phiên xác thực nhiều người dùng với đủ các vai trò được xác thực bằng vân tay thông qua đầu đọc vân tay. Nếu điều kiện xác thực không hợp lệ (không đủ vai trò, không đủ số lượng người dùng trong một phiên xác thực) hệ thống sẽ kích hoạt tín hiệu đầu ra điều khiển thiết bị cảnh báo.

2) Cảnh báo cục bộ và trung tâm

Nếu điều kiện xác thực không hợp lệ, thiết bị điều khiển kích hoạt tín hiệu đầu ra điều khiển thiết bị cảnh báo và gửi bản tin cảnh báo đến ứng dụng được cài đặt trên máy chủ trung tâm. Bản tin cảnh báo chứa đầy đủ thông tin về vị trí cảnh báo, người dùng truy cập, thời gian xảy ra cảnh báo, trạng thái đầu vào khác. Trao đổi thông với thiết bị sử dụng các giao thức truyền thông chuẩn phổ biến như: TCP, UDP, HTTP, RESTful Web Services, v.v..

3) Ghi thông tin theo dõi cục bộ

Thiết bị phần cứng cho phép ghi lại thông tin các lần truy cập thiết bị trong trường hợp mất kết nối truyền thông. Khi có kết nối truyền thông, thiết bị tự động gửi các thông tin đã lưu lên ứng dụng được cài đặt trên máy chủ trung tâm.

4) Hỗ trợ tối đa 8 vân tay cho mỗi người dùng

Hệ thống theo sáng chế cho phép mỗi người dùng đăng ký tối đa 8 vân tay.

5) Hỗ trợ tối đa 100 người dùng.

6) Thêm, sửa, xóa, gán vai trò người dùng

Hệ thống theo sáng chế cho phép đăng ký người dùng mới, sửa thông tin hoặc xóa người dùng đang tồn tại và gán vai trò cho người dùng.

7) Đăng ký liên tục trong một phiên đăng ký

Thiết bị cho phép đăng ký liên tục nhiều vân tay cho một người dùng và nhiều người dùng trong một phiên đăng ký.

8) Bảo mật bằng mật khẩu

Hệ thống theo sáng chế yêu cầu mật khẩu khi người dùng truy cập các chức năng cấu hình và mật khẩu có thể thay đổi được bởi người dùng quản trị thông qua bàn phím trên thiết bị hoặc thông qua giao diện quản trị web.

9) Cấu hình thông qua giao diện web

Hệ thống theo sáng chế cung cấp giao diện web cho phép cấu hình từ xa thiết bị. Các tham số cấu hình như: Địa chỉ MAC, địa chỉ IP, mức bảo mật, mở/khóa bàn phím thiết bị, cho phép/không cho phép tắt tín hiệu đầu ra điều khiển cảnh báo trên bàn phím thiết bị, thiết lập thời gian hệ thống, thiết lập khoảng thời gian tối đa cho phiên xác thực.

10) Hủy phiên xác thực

Hệ thống theo sáng chế sẽ hủy phiên xác thực nếu người dùng xác thực vân tay nhưng không có tín hiệu đầu vào điều khiển kết thúc phiên xác thực sau một khoảng thời gian được cấu hình trước.

11) Bảo toàn dữ liệu khi mất điện

Các dữ liệu cấu hình, người dùng, thông tin theo dõi cảnh báo vẫn tồn tại khi mất nguồn điện cấp cho thiết bị.

12) Màn hình hiển thị thông tin

Hệ thống theo sáng chế sử dụng bộ phận hiển thị, ví dụ, màn hình LCD 4 hàng x 12 cột cho phép hiển thị thông tin cơ bản.

13) Kiểm tra tình trạng kết nối mạng

Hệ thống theo sáng chế cung cấp công cụ kiểm tra tình trạng kết nối mạng của các thiết bị khác như camera, máy tính v.v..

Trong các đặc điểm chức năng nêu trên, các đặc điểm kỹ thuật quan trọng của hệ thống điều khiển truy cập thông qua quy trình xác thực vân tay đồng thời nhiều người dùng với nhiều vai trò khác nhau theo sáng chế sẽ được thể hiện rõ hơn dưới đây.

Một trong các ưu điểm của hệ thống theo sáng chế là nâng cao độ an toàn thông qua việc yêu cầu xác thực hợp lệ khi đồng thời nhiều người dùng với nhiều vai trò đồng thời được xác thực bằng vân tay.

Đặc điểm chức năng này được thực hiện thông qua thuật toán được cài đặt trong phần sụn (firmware) của thiết bị phần cứng xác thực vân tay.

Mỗi người dùng được gán một vai trò xác định đại diện bởi định danh của vai trò. Định danh của vai trò là một số nguyên dương nhận giá trị trong khoảng từ 0 đến $N-1$ trong đó N là một số nguyên dương được cấu hình trước. Giá trị mặc định của N trong hệ thống, ví dụ, là $N=5$.

Danh sách vai trò yêu cầu cho cho xác thực hợp lệ là một mảng N phần tử gọi là *MangVaitroYeucau* trong đó mỗi phần tử nhận một trong hai giá trị đúng (*True*) hoặc sai (*False*). Giá trị *True* của một phần tử có nghĩa là vai trò có định danh tương ứng là chỉ số mảng của phần tử đó cần trong xác thực hợp lệ. Giá trị *False* của một phần tử có nghĩa là vai trò có định danh tương ứng là chỉ số mảng của phần tử đó không cần trong xác thực hợp lệ. Giá trị của các phần tử trong *MangVaitroYeucau* được định nghĩa trước tùy thuộc vào yêu cầu của từng hệ thống. Khi có nhiều hơn 01 phần tử của mảng *MangVaitroYeucau* được thiết lập giá trị *True* có nghĩa là nhiều (đa) vai trò cần được xác thực bởi hệ thống.

Danh sách vai trò thực tế có được trong một phiên xác thực là một mảng N phần tử gọi là *MangVaitroThucte* trong đó mỗi phần tử nhận một trong hai giá trị *True* hoặc *False*. Khi bắt đầu một phiên xác thực, các phần tử của mảng *MangVaitroThucte* được thiết lập về giá trị *False*. Trong một phiên xác thực, khi một người dùng xác thực có vân tay trùng khớp với một dữ liệu vân tay trong cơ sở dữ liệu, định danh tương ứng của vai trò của người dùng (*RoleID*) được dùng như chỉ số mảng để cập nhật phần tử tương ứng của mảng *MangVaitroThucte* thành giá trị *True* ($MangVaitroThucte[RoleID] = True$). Khi nhận được tín hiệu điều khiển đầu vào kết thúc phiên xác thực, hai mảng *MangVaitroYeucau* và mảng *MangVaitroThucte* được so sánh với nhau. Nếu 2 mảng có tất cả các phần tử giống nhau thì phiên xác thực là hợp lệ. Lưu đồ thuật toán này được minh họa trong Hình 3.

Ưu điểm khác của hệ thống theo sáng chế là nâng cao độ an toàn thông qua việc chức năng bắt hợp lệ phiên xác thực sau một khoảng thời gian cho trước.

Thời gian xác thực hợp lệ cho một phiên xác thực được cấu hình trước và lưu trong bộ nhớ của thiết bị ký hiệu là *ThoigianXacthucHople*. Khi bắt đầu phiên xác thực thời gian bắt đầu của phiên xác thực được lưu bằng thời gian của hệ thống tại

thời điểm hiện tại ký hiệu là *ThoigianBatdauXacthuc*. Trong vòng lặp của phiên xác thực, thời gian hiện tại của hệ thống ký hiệu là *ThoigianHientai* được lấy. Nếu $ThoigianHientai - ThoigianBatdauXacthuc > ThoigianXacthucHople$ thì dừng phiên xác thực.

Cần hiểu rằng, phần nêu trên chỉ thể hiện một phương án thực hiện sáng chế. Mặc dù sáng chế đề xuất hệ thống điều khiển truy cập thông qua quy trình xác thực vân tay đồng thời nhiều người dùng với nhiều vai trò khác nhau, nhưng với nguyên lý của sáng chế như được thể hiện ở đây, sáng chế hoàn toàn có thể được thực hiện dưới dạng phương pháp điều khiển truy cập hoặc chương trình điều khiển truy cập tương ứng. Ngoài ra, các khía cạnh của sáng chế có thể được sử dụng, thay thế với các khía cạnh bất kỳ khác để tạo ra các dạng thay đổi, cải biến của sáng chế. Các dạng thay đổi, cải biến này cũng không nằm ngoài phạm vi của sáng chế.

YÊU CẦU BẢO HỘ

1. Hệ thống điều khiển truy cập thông qua quy trình xác thực vân tay đồng thời nhiều người dùng với nhiều vai trò khác nhau, hệ thống này bao gồm:

các thành phần phần cứng bao gồm:

bo mạch chủ xử lý bao gồm bộ chip vi điều khiển và các vi mạch IC phụ trợ thực hiện các chức năng giao tiếp mạng, điều khiển vào ra và giao tiếp với các đầu đọc vân tay, các thuật toán xử lý được lập trình và nạp vào trong bộ nhớ ở bên trong chip vi điều khiển;

mô đun đầu đọc vân tay được sử dụng để đọc vân tay và lưu giữ các vân tay của người sử dụng, các thuật toán so sánh các đặc trưng vân tay được cài đặt trong mô đun này;

màn hình hiển thị để hiển thị thông tin tương tác với người dùng;

loa của thiết bị để phát các âm thanh cảnh báo, âm bàn phím, âm chỉ thị;

bàn phím dùng để nhập các thông tin và giúp người dùng tương tác với thiết bị phần cứng;

các cổng điều khiển vào ra dùng để điều khiển các thiết bị cảnh báo bên ngoài và nhận tín hiệu điều khiển đầu vào;

cổng giao tiếp mạng dùng để cắm dây mạng để kết nối thiết bị vào mạng truyền thông;

máy chủ trung tâm được cài đặt ứng dụng giao diện web, truyền thông qua mạng với bo mạch chủ xử lý để có thể giám sát và cấu hình từ xa bo mạch chủ và các thiết bị phần cứng khác;

thành phần phần mềm được cài đặt trong các thành phần phần cứng tương ứng để thực hiện các bước sau đây:

xác thực hợp lệ khi đồng thời nhiều người dùng với nhiều vai trò đồng thời được xác thực bằng vân tay thực hiện thông qua thuật toán được cài đặt trong phần sụn (firmware) của thiết bị phần cứng xác thực vân tay, trong đó:

mỗi người dùng được gán một vai trò xác định đại diện bởi định danh của vai trò, định danh của vai trò là một số nguyên dương nhận giá trị trong khoảng từ 0 đến $N-1$, trong đó N là một số nguyên dương được cấu hình trước,

danh sách vai trò yêu cầu cho việc xác thực hợp lệ là một mảng N phần tử gọi là `MangVaitroYeucau`, trong đó mỗi phần tử nhận một trong hai giá trị đúng (True) hoặc sai (False), giá trị True của một phần tử có nghĩa là vai trò có định danh tương ứng là chỉ số mảng của phần tử đó cần trong xác thực hợp lệ, giá trị False của một phần tử có nghĩa là vai trò có định danh tương ứng là chỉ số mảng của phần tử đó không cần trong xác thực hợp lệ, giá trị của các phần tử trong `MangVaitroYeucau` được định nghĩa trước tùy thuộc vào yêu cầu của từng hệ thống,

danh sách vai trò thực tế có được trong một phiên xác thực là một mảng N phần tử gọi là `MangVaitroThucte`, trong đó mỗi phần tử nhận một trong hai giá trị True hoặc False, khi bắt đầu một phiên xác thực, các phần tử của mảng `MangVaitroThucte` được thiết lập về giá trị False, trong một phiên xác thực, nếu một người dùng xác thực có vân tay trùng khớp trong cơ sở dữ liệu, thì định danh tương ứng của vai trò của người dùng (RoleID) được dùng làm chỉ số mảng để cập nhật

phần tử tương ứng của mảng MangVaitroThucte thành giá trị True (MangVaitroThucte[RoleID] = True), khi nhận được tín hiệu điều khiển đầu vào kết thúc phiên xác thực, hai mảng MangVaitroYeucan và mảng MangVaitroThucte được so sánh với nhau, nếu 2 mảng có tất cả các phần tử giống nhau thì phiên xác thực là hợp lệ; và

bất hợp lệ phiên xác thực sau một khoảng thời gian cho trước, trong đó thời gian xác thực hợp lệ cho một phiên xác thực được cấu hình trước và lưu trong bộ nhớ của thiết bị.

2. Hệ thống điều khiển truy cập theo điểm 1, trong đó khi điều kiện xác thực không hợp lệ, hệ thống này kích hoạt tín hiệu đầu ra điều khiển thiết bị cảnh báo cục bộ và gửi bản tin cảnh báo đến ứng dụng được cài đặt ở máy chủ trung tâm, bản tin cảnh báo này chứa thông tin về vị trí cảnh báo, người dùng truy cập, thời gian xảy cảnh báo, trạng thái đầu vào khác, việc gửi bản tin được thực hiện bằng cách truyền thông sử dụng một hoặc một số giao thức truyền thông chuẩn phổ biến bao gồm TCP, UDP, HTTP, RESTful Web Services.

3. Hệ thống điều khiển truy cập theo điểm 1, trong đó hệ thống này có chức năng ghi thông tin theo dõi cục bộ trong bộ nhớ của bo mạch chủ xử lý, thông tin này là thông tin về các lần truy cập thiết bị trong trường hợp mất kết nối truyền thông, khi có kết nối truyền thông, thiết bị tự động gửi các thông tin đã lưu lên ứng dụng được cài đặt trên máy chủ trung tâm.

4. Hệ thống điều khiển truy cập theo điểm 1, trong đó hệ thống này có chức năng hỗ trợ tối đa 8 vân tay cho mỗi người dùng.

5. Hệ thống điều khiển truy cập theo điểm 1, trong đó hệ thống này có chức năng hỗ trợ tối đa 100 người dùng.

6. Hệ thống điều khiển truy cập theo điểm 1, trong đó hệ thống này có chức năng thêm, sửa, xóa, gán vai trò người dùng.

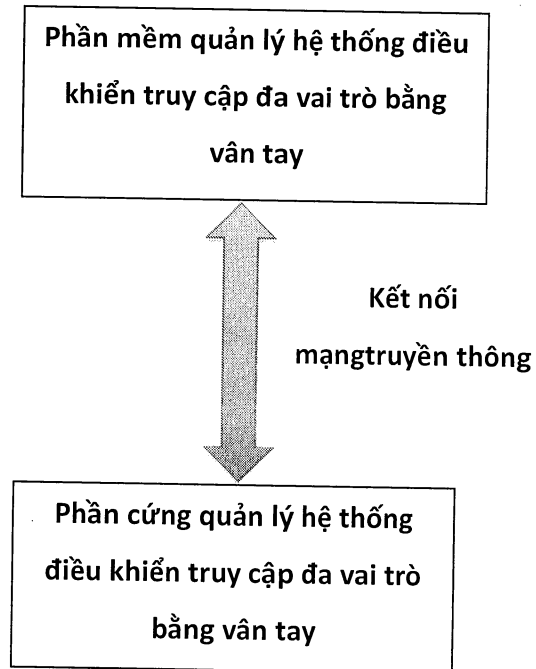
7. Hệ thống điều khiển truy cập theo điểm 1, trong đó hệ thống này có chức năng đăng ký liên tục nhiều vân tay cho một người dùng và nhiều người dùng trong một phiên đăng ký.

8. Hệ thống điều khiển truy cập theo điểm 1, trong đó hệ thống này có chức năng bảo mật bằng mật khẩu, hệ thống theo sáng chế yêu cầu mật khẩu khi người dùng truy cập các chức năng cấu hình và mật khẩu có thể thay đổi được bởi người dùng quản trị thông qua bàn phím trên thiết bị hoặc thông qua giao diện quản trị web.

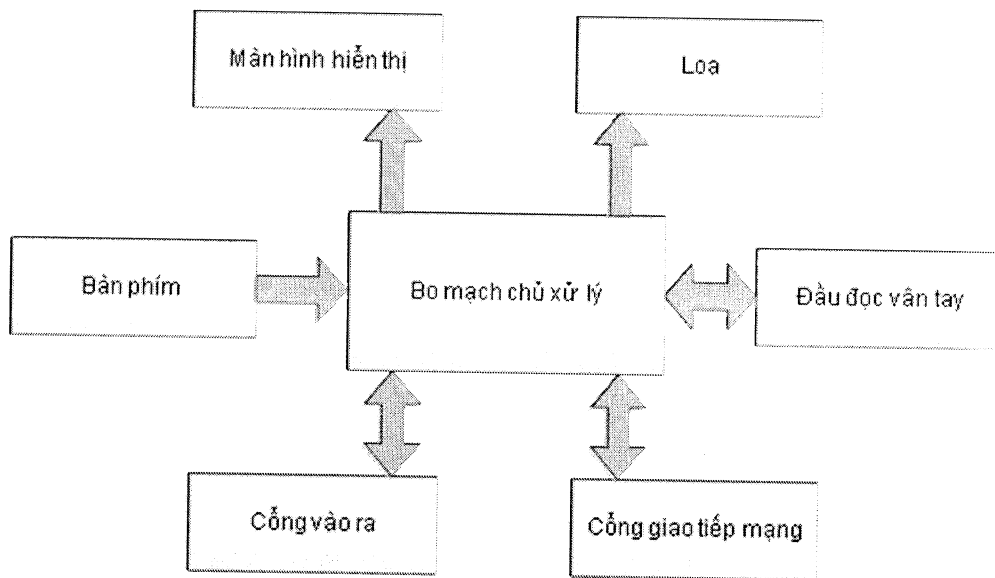
9. Hệ thống điều khiển truy cập theo điểm 1, trong đó hệ thống này cung cấp chức năng cấu hình thông qua giao diện web cho phép cấu hình từ xa thiết bị, các tham số cấu hình bao gồm: địa chỉ MAC, địa chỉ IP, mức bảo mật, mở/khóa bàn phím thiết bị, cho phép/không cho phép tắt tín hiệu đầu ra điều khiển cảnh báo trên bàn phím thiết bị, thiết lập thời gian hệ thống, thiết lập khoảng thời gian tối đa cho phiên xác thực.

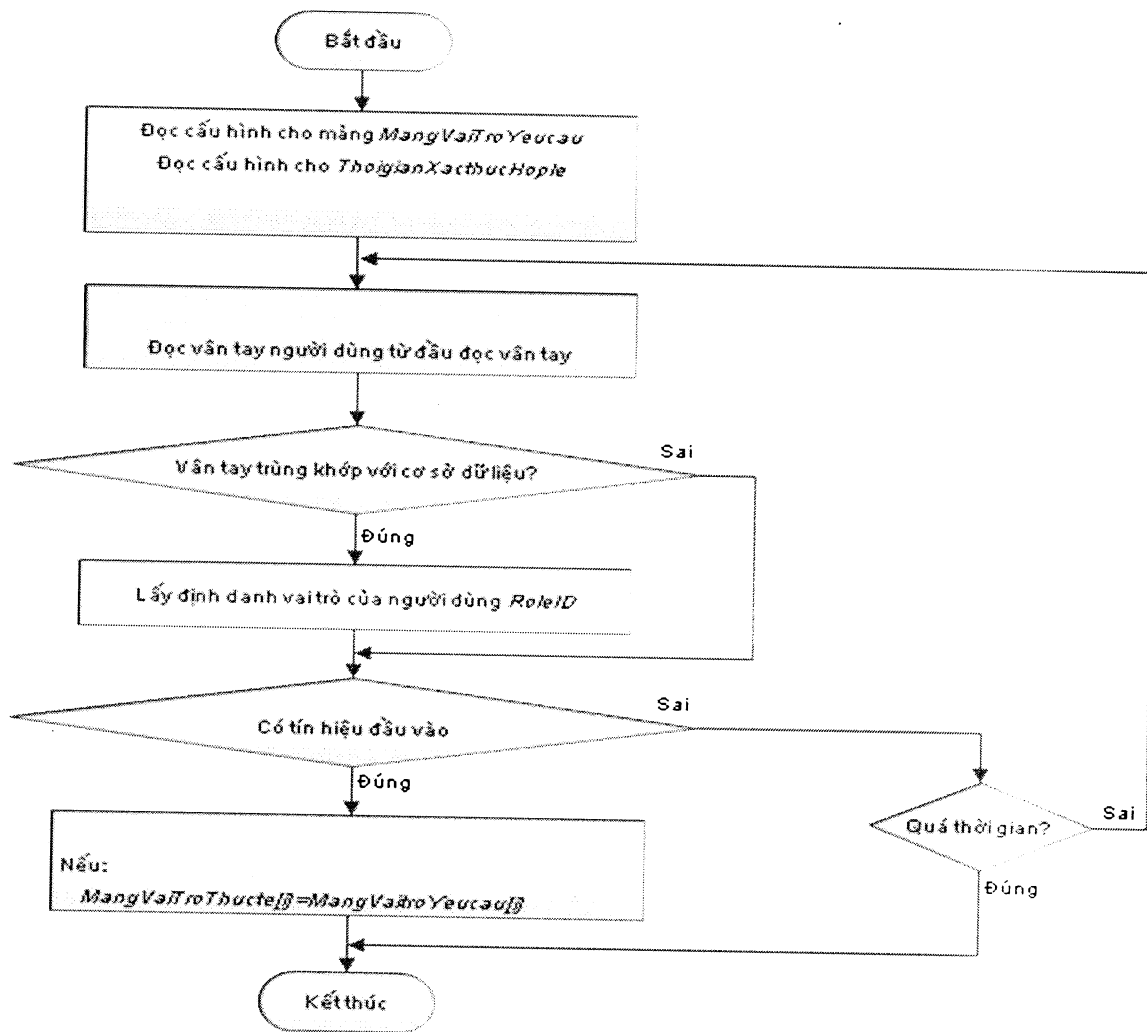
11. Hệ thống điều khiển truy cập theo điểm 1, trong đó hệ thống này có chức năng bảo toàn dữ liệu khi mất điện, các dữ liệu cấu hình, người dùng, thông tin theo dõi cảnh báo vẫn tồn tại khi mất nguồn điện cấp cho thiết bị.

12. Hệ thống điều khiển truy cập theo điểm 1, trong đó hệ thống này có chức năng kiểm tra tình trạng kết nối mạng của các thiết bị phần cứng khác khác như bo mạch chủ xử lý, camera, máy tính, và các thiết bị cần nối mạng trong hệ thống.



Hình 1

**Hình 2**



Hình 3